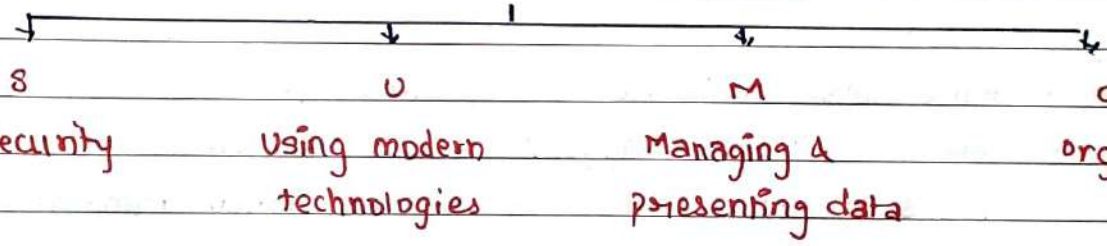
__/__/____

9. DATA GOVERNANCE.

INTRODUCTION:

1. Data Governance encompasses all efforts to ensure data security, privacy, accuracy, availability, useability.
2. DG manages → availability, useability, integrity & security of data.
3. operates on internal data standards & policies
4. There are various companies alleged for data Breaching like Equifax, Facebook, Yahoo.

Data Governance is divided into 4 parts.



Principles of DG [MAD TCS2]

1. Maintaining the integrity of data:
   - use data in an appropriate manner.
   - means and goals shall be ethical
   - participants shall be honest.
2. Transperancy:
   - proper ~~technology~~ transperancy shall be maintained.
   - parties must understand how it is utilized
   - useage of data shall be authorized by all involved parties

__/__/____

3. Accountability and ownership of data:
- ownership shall be defined
- procedures shall be followed for proper access of data.

4. Data Audit:
- Audit can be done on every phase of DG.
+ Any decision, control, process

5. Change in Management:
- There are discrepencies in data, it can never be 100% accurate
- DG ensures proper change in mgmt activities to acheive proper accuracy in data.

6. Stewardship [Leadership]:
- must follow principle of stewardship.
- every org" shall appoint a data steward.
- He shall follow the best practice when managing data.

7. Standardization of data:
- data is used by many teams so the format of data presentation → shall be standardize.

Importance of Data Governance:

1. Better Analysis
2. Easily defined goals
3. Consistent compliance
4. Improved Data mgmt.
5. Standardize System
6. Improved data quality.

__/__/____

CHALLANGES OF DATA GOVERNANCE:

1. Understanding the business value of DG:

- Challenge:
  - → convincing the organisation of business value beyond data speed.
  - → co. prefer faster data & compromise over quality or source.

- Solution:
  - → Appointment of a cheif Data Officer (CDO)
  - → Form an Analytics Group: They will highlight the -ve impact of poor data on decision making.

2. Perception of IT owns the data:

- Challenge:
  - → There's a misconception → that data only belongs to IT department and no other department.
  - → But IT dept is not involved in all aspects of orgⁿ.

- Solution:
  - → Define clear data ownership.
  - → Shift DG to all aspects | dept of orgⁿ.
  - → The dept manager shall own & manage data usage.
    eg: sales data belongs only to sales team.

3. Limited or misallocated resources:

- Challenge:
  - → lack of dedicated resources or misallocation of existing one for data owner.

- Solution:
  - → conduct internal training for existing employees.

__/__/____

→ hire DG expert from consulting firms
→ orgⁿ shall invest in dedicated data owner.

4. Lack of data control:

• Challenge:
→ overly restricted data security measures hampers data utilization and value creation.
→ misplaced focus of team members.
→ lack of understanding.
→ fear of misuse

Solution:
→ implement DG practice to gain deep knowledge
→ use various tools to map data assets.
→ Prioritise data security w/o suffocating its potential value

5. Poor data context:

• challenges:
→ Lack of trust in data
→ ie not poor quality but lack of clarity
→ Lacks clarification
→ misrepresentation of data.

Solution:
→ percepton shall be improved by team members
→ implement a feedback loop for users to communicate queries.

__/__/____

DIFFERENCE BETWEEN

	DATA GOVERNANCE	DATA MANAGEMENT.
Definition:	→ process of ensuring → business rules for data are established & followed.	→ making sure that all data is captured, managed, used & disposed of properly.
Scope:	→ ensures quality of data & its mgmt process	→ ensure that all data have been collected, stored, managed.
Benefits:	→ more effcient by providing a framework for managing data. → ensures effeciency, consistency in project → reduces errors.	→ improves effeciency, accuracy, and security of data.
challenges:	→ hard to know where you should start your data governance process. → resistance from employees who don't want their work interrupted by new rules.	→ ~~one set~~ there is no one set std for how data should be organised & stored.
Best Practices	→ Many best practices: → proper classification of data. → use of access control lists to grant/deny access	→ good life naming → high quality of data, → proper labelling → secure data storage.
Technology:	→ can be used to automate processes → improve the effectiveness of current processes.	→ Data bases Mgmt system → Data mining tools → Data visualization Tools → Big data Technologies.

__/__/____

EFFECTIVE DATA GOVERNANCE FRAMEWORK.

1. Common objective → of DG
Standardization of data accross the organisation.

2. Every org^n is guided by certain business drivers such drivers dictates what need to be carefully controlled

3. Example: for a health care org^n → business driver is the patient's data which needs to be protected.

4. So a well planned DG framework covers strategic, tactical, operational roles.

IMPORTANCE OF DG FRAMEWORK.

→ gives consistent view of data, with flexibility for needs of individual business units.

→ ensures data quality, accuracy completeness and consistency.

→ An ability to understand data increases along with making data discoverable useable and easier to connect ensures 'single version of the truth' i.e it keeps artificial issuer align with enterprise.

→ Best practices can be applied across the org^n

→ Ease to keep data secure, complaint and confidential as per law.

__/__/____

3 PILLARS OF DATA GOVERNANCE

1. Governance includes all data Assets:

→ dash board and code to data science all one data assets.

→ DG framework shall take into account all data Assets.

2. Practitioners led or Bottom up Approach:

→ As no. of data increases Accountability on few people for data with hamper the ~~Stability~~ scalability of the business.

→ so a decentralized approach Bottom up, DG where every data creator is responsible for DG is a new way forward.

(a) Top down Approach (Data control)

- centralised Approach
- Small team.

Advantages: - Has whole control
- No misuse

disadvantages: - ~~scability~~ scalability issues
- controls makes process rigid.
- small team gets overburdened.

(b) Bottom up Approach [data Access]

- Decentralised
- huge organisation

Advantages: - Scalable

Disadvantages: - Misuses
- risks regulatory
- lack of stakeholders trust.

131

__/__/____

(c) Border Approach

- mixture of < Access control.

Advantages: - Agility of bottom up + necessary governance to mitigate unregulated data entry.

3. Governance practice shall be embedded within daily workflows.

STEPS INVOLVED IN CREATING DATA GOVERNANCE FRAMEWORK.

1. Revisiting the definition governance:

→ Data governance is an ever-evolving project which required to re-visit.

→ Following questions needs to ~~to~~ be followed on:

(a) purpose kya hai?

(b) data assets saare covered hai?

(c) data sharing ho rahi hai? between departments.

2. Identification and defining data domain.

- standardise data domains across whole organisation.
- ~~Soo~~ sawal:
  - (a) Imp domain konse hai?
  - (b) which data is generated?
  - (c) Kaha rakha hai data?
  - (d) Kon consume kar raha hai?

3. Identify data owners and consumer.

- each domain creating data is responsible for managing data and securing it
- Right people shall have access.

__/__/____

- sawaal:
  a) Kon consume kar raha hai?
  b) dept ki aapas mai dependencies hai kay? for data?
  c) Kon create kar rahi data?

4. Validating and documenting everything pertaining to data:
→ org^n shall follow & document proper flow rules and workflows of DQ.
→ sawaal:
  a) data originate from?
  b) What does it mean?
  c) Flow kya hai?
  d) goals achieve ho rahe hai?

5. Conducting data security & risk assessment:
→ Each data must be secured properly and continuously look after identification and assessment of risk.
→ a) existing policy and security kya hai?
  b) Who can access data?
  c) Policies kya risk mitigate karti hai?

DQQI THEMES

1. Data Generation:
- Focus: Effeciently generating useful data during program implementation
→ Key points:
- Digitization: level of digital records
- Frequency: How often data is updated
- Granularity: How detailed the data is.
- Tools: Use of mobile phones, location tracking, GIS for data authentication.

__/__/____

2. Data Quality :

Key Points
- Focus: Ensuring data meets quality benchmarks.
- Processes: Data profiling, cleaning, quality checks.
- Tools: Modern technologies like mobile phones & automated pipelines.
- Standards: Proper design (schemas) for data pipelines.

3. Use of Technology:

Key Points:
- Focus: Leveraging new tech for better data handling.
- Integration: Linking MIS with systems like PFMS & JAM (Jan Dhan-Aadhar Mobile).
- Sources: Use of Remote sensing, social media, etc.
- Emerging Tech: Block chain, AI, IoT, Big Data Analytics for insights.

4. Data Analysis, Use & Dissemination:

Key Points:
- Focus: Using data for decisions & sharing results.
- Analysis: Basic (cross-sectional) & advanced (predictive / regression).
- Dashboards: Visualising data for easy understanding.
- Accessibility: Websites with multi-lingual support & social media integration.

5. Data Security & HR Capacity:

Key Points:
- Focus: Protecting data and improving staff capacity.
- Security: Antivirus, internal audits to prevent ~~sour~~ corruption / threats.
- HR: Dedicated teams for data quality improvement.

6. Case Studies:

Focus: Learning from innovative practices

Key Points:
- Best Practices: Highlighting Success Stories
- Collaboration: Promoting inter-ministry teamwork.

__/__/____

SECTOR WISE DATA GOVERNANCE SCENARIO :

I] AUTOMOBILE INDUSTRY

⇒ Data Collection & Management in Connected & Automated Vehicles.

a) Approaches to Data Collection & Mgmt at Vehicle level.

→ Vehicles collect Personal data about drivers and passangers (eg: movement Vehicle condition)

→ Privacy risks are addressed through data protection principles made by public & private sectors.

b) Data Processing in Vehicles.

→ Where & how data is processed depends on technical & regulatory needs.

→ Data is shared among manufachurers, regulators, cloud services & third party providers.

⇒

c) Access to Vehicle data:

→ Who controls the data?

→ Manufacturers control data after getting consent from the owner/driver.

→ Consent is needed for using the vehicle & its services.

→ debate: • Manufactures prioritize security & privacy
• others (eg, repair/service providers) want data access for competition.

d) Data Sharing & Access Models

→ Data benefits many, like:
- Automative industry (manufachuring, repairs)
- Third parties (entertainmen

→ Data sharing can speed up innovation in automated vehicles.

→ Challanges:
- Data is reusable, making markets tricky.
- New frameworks are needed to promote sharing among industry players.

__/__/____

c) Data Reporting & Mandatory collection:

→ Why collect data?

→ Helps in policy making (eg transport, safety).

→ Improves road operations, safety & planning.

II] ENERGY SECTOR:

1. Data Explosion & Innovation vs Regulation.

→ Energy companies collect vast amount of data daily from devices like meters & senors.

Challenges:
1. Balancing innovation (eg AI, IOT, ML) with privacy laws, & regulatory mandates.
2. Risk of uninkntionally violating data protection laws due to rapid technology adoption.

Key issue: Regulatory bodies must ensure a balance: over regulation hampers growth; under regulation undermines trust.

2. Poor data Governance in the Energy Sector:

Current State:
- Many power cos fail to fully utilize data or meet modern data-sharing needs.
- Lack of formal data strategies for emissions reporting, sustainability and operational effeciency.

Data dependancy:
- Accurate data is crucial for:
  - → Grid reliability, cost efficiency, financial Reporting.
  - → Planning for peak energy demands, storm preparedness, and disaster mitigation.
  - → Data should be an asset for future growth, not just a tool to avoid issues.

__/__/____

3. Survey insights (EY Report)

→ Few energies companies have a chief Data officer. (CDO)

→ Less than 1/3rd have formal data strategy serving both IT & business needs.

Recommendat^{n}: → Establish formal data oversight. eg data governer

→ Create a single source of truth for all data, accessible across business functions.

→ Anticipate future compliance needs. (eg renewable energy integration, climate change strategies).

4. Questions to build a Strong Data Strategy.

Energy companies should consider the following when formulating a robust data strategy.

1. Data Quality : How will you measure & ensure high data Quality ?
2. Stakeholder Involvement : Are senior ~~ta~~ leaders , IT teams , and key stakeholders actively involved ?
3. Sustainability Trends : Have ESG trends been identified & addressed ?
4. Data Access : Does the strategy ensure the right data is accessible to users at the right time?
5. Self Service Analytics : Is there a plan to employer business users with analytics capabilities ?
6. Stakeholders Expectations: How can stakeholder needs be understood and met effectively?
7. Data as an Asset : How can data be treated as the organisations most valuable product ?

__/__/____

III.] HOSPITALITY INDUSTRY:

1. Complex Ownership Structures:

- Issue: - Hotels and restaurants often have multiple owners. (franchise)
- • Each group uses different computer systems & data frequently moves between them.
- Example: Wyndham Worldwide breach (2008-2010)
  - Hackers guessed weak passwords of one operator's system.
  - Spread across the network compromising 619,000 customer data.

2. Payment via cards:

- Issue: Heavy reliance on credit/debit cards for reservations and payments.
  Hackers target POS (point of Sale) to steal card details.
- Example: out of 21 major data breaches since 2010, 20 involved malware in POS systems.
- Malware spreads across multiple hotels and can remain undetected for months.

3. High Staff Turnover:

- Issue: • Hospitality industry relies on seasonal staff, leading to frequent job changes.
  - Well trained staff are essential to protect data & recognise scams.
  - High T~~o~~T/o creates challenges in maintaining trained teams.
- Risk: Untrained staff may unintentionally allow hackers access to sensitive data.

__/__/____

4. Compliance:
- Issue: Strict laws require secure handling of customer data.
- Key Regulations:
  - GDPR (EU, 2018) Protects personal data & enforces stricter rules on its storage.
- Risk: Non-compliance can result in huge fines, damaging the company's reputation & survival.

5. Insider Threats:
- Issue: Employees may sell customer data to third parties. Data comes from interactions on website, booking systems & reviews. Such data is valuable to competitors & could be misused for profit.

IV.] TELECOM SECTOR:

⇒ Telecom sector needs to embrace a successful telecom. data governance which is built on following 4 pillars:

1. Link Data Governance to Business Goals.
2. Prioritise data sets to be governed based on the business value they provide.
3. Engage & communicate value to strategic, operational & tactical teams.
4. Leverage cultural engagement process & people to reinforce data governance value on a day to day basis.

⇒ Telecom DG in India → TRAI recomends an Apex Body for DG:

1. TRAI recommends forming the DDMC Data Digitization & Monetizat^{n} Council as an apex body to address data related issues in India.
2. DDMC → oversee the ethical use of data by both govt & corporates
3. DDMC → will have representation from Dept of Telecom. (DoT) & Ministry of Electronics & IT (MEIT).

__/__/____

I] Ecommerce SECTOR:

⇒ These insights have a huge part to play in:

1. Informing gaps to adapt to consumer & market trends
2. More effective customer retention & engagement.
3. Optimization of pricing, inventory and labour allocations.
4. Informing innovation as well as new and untapped market opportunities.

Significance of DG in E-Commerce:

1. Visibility, Relevance, consistency.
2. Limiting Data Exposure
3. Dealing with Data inconsistencies

(write andar ka masala on your own)

Merits of DG in E-commerce:

1. Overall performance:

→ DG → boosts e-com effeciency → Saves time & enabling teams to access accurate data quickly, improving overall biz performance.

2. Data Quality:

→ tracks data quality and usage metrics, giving cos. visibility into how data is used to accross teams.

3. Better Business Insights:

→ Analytics enabled by DG help identify performance gaps, discover new revenue streams, & gain a competitive advantage.

4. Improved Decision-Making:

→ with high-quality data e-com cos can make quicker, accurate decisions while maintaining privacy & compliance

5. Data ownership, Responsibility & Accountability:

→ Data governance clarifies ownerships & accountability, allowing teams to effectively manage & share data with clear contacts for issues & expertise.

__/__/____

VI] BANKING SECTOR.

Key Value Propositions of Data Governance in Banking.

i) regulatory compliance:

- Ensures that Banks adhere to federal & state regulatⁿˢ for data security.
- Helps banks manage data location, access & security, particularly during digital transformation projects like cloud migrations.

ii) Cost cutting:

- Reduces the inefficiency of manual data mgmt by centralizing data governance cutting down on costly IT teams & third-party systems.
- Self-service capabilities of DG tools ensure secure & efficient data access.

iii) Market insights:

- supports data analysis, enabling banks to gain actionable insights & remain competitive.
- Encourages company-wide data access & organization, facilitating innovation across the bank.

iv) Data-driven culture:

- Promotes a data-driven approach that enhances cost-cutting innovation & customer insights.
- Encourages more effective operations & customer-focused decision making.

v) collaboration & Risk Mgmt:

- facilitates data discovery, quality assessment, & cataloging, improving collaborat^{n}, decision-making & productivity.
- Helps manage customer acquisition, fraud detection & risk reduction.

vi) Improved compliance & customer service:

- Enhances customer experience by integrating secure data controls, supporting compliance & less intrusive data handling.
- Personalised experiences are enabled by overcoming challenges of segmented data.

__/__/____

Embedding ESG into core Banking Processes:

1. Integrating new workflows into existing processes.
2. Communication of ESG requirements across the organisation.
3. Review & revise existing data processes to comply with changing ESG requirements.
4. Developing a clear plan to support the integration of new ESG policies.

IMPORTANT REGULATORY DIMENSIONS.

I. IT (Reasonable Security Practices & Procedures & Sensitive Personal data or Information) Rules, 2021.

- **Privacy Policy Requirement:**

→ The body corporate or any person handling personal information on behalf of the body corporate must provide a privacy policy for handling personal & sensitive personal data.

- **Accessibility:**

- The policy must be available for review by those who provided the information under a lawful contract.

- **Publication:**

The privacy policy must be published on the body corporate's website or on the website of any person handling the data on its behalf.

- **Policy contents:**

1. clear & accessible statements of data handling practices & policies.
2. Types of personal or sensitive personal data collected.
3. Purpose of collecting & using the data.
4. Disclosure practices, including sensitive data.
5. Reasonable security practices for protecting the data.

__/__/____

- Personal information Definition:

Personal info' refers to any data, that identifies a natural person, either directly or indirectly, when combined with other available information.

- Sensitive Personal Data: includes:

1. Passwords
2. financial info (bank A/c)
3. Health & medical details.
4. (physical, physiological, mental health, medical history)
4. Sexual orientation
5. Biometric info
6. Any details related to the above provided by the individual or processed by the body corporate.

- Exclusions from Sensitive Data:

- Info freely available in the public domain or under the Right to Info Act, 2005 is not considered sensitive personal data.

DIGITAL PERSONAL DATA PROTECTION ACT, 2023.

* Assent & Purpose: - The act received the assent of President on 11/08/2023
- It governs the processing of digital personal data, balancing individuals' right to privacy with the need for lawful data processing.

* Scope of the Act:

1. Domestic Applicability: Applies to the processing of digital personal data within India, whether data is collected in digital or non-digital form (once digitized).

2. International Applicability: Also applies to processing outside India if it relates to offering goods or services to data principles in India.

__/__/____

exemptions: the act does not apply to:

- Personal data processed by individuals for personal or domestic use.
- Data made publicly available by the data principal or by any person as per legal obligations.

- General obligations of data Fiduciaries: Data fiduciaries must adhere to obligations regarding the processing of personal data.
- Children's Data: special focus on the processing of personal data of children.
- Additional obligations for significant Data fiduciaries: certain entities may have additional obligations due to their impact on data processing.
- Rights of Data Principals: includes rights to access personal data, grievance redressal & more.
- Duties of Data Principals: Outlines responsibilities for individuals (data principals) providing personal data.

→ Data Governance: to ensure its success, an organization needs a way to measure its progress & identify areas for improvement.

→ The three maturity levels that organisations go through as they become more data-driven companies are:

1) Data integration: application integration, data integration, & data loading.
2) Data integrity: data preparation, data stewardship, & data quality
3) Data intelligence: data cataloging, data lineage, & metadata mgmt.